REMARKS

Applicant has amended the claims to more specifically define applicants invention. Applicant's invention is directed to a dual mode of authentication and the amendments have clarified the type of fingerprint that is created in applicant's invention. The fingerprint created in Applicant's invention is a digital fingerprint of one or more components of a user's computer. The support for these amendments may be found at the following locations in the application:

Page 14, lines 6-9 where the inventor states:

> "At that point, the apply.asp "reads" diagnoses whether the user's PC has labelled certain components which can be used for generating a fingerprint file for helping to verify user's PC's identity in future functions..."

Page 14, lines 21-25 where the Applicant states:

> "Activation of the account also initiates a process by which the Creditor Toolbox generates a fingerprint file including a unique identification ("UID") for the user using the identifying characteristics of user's PC which were diagnosed by the apply.asp and accompanied the application (e.g. CPU ID number, hard disk serial number, amountg[sic] of RAM, BIOS version and type, etc.)"

There is also support at Page 17, lines 10-13.

> "The form is accompanied transparently by the fingerprint file containing the UID and other machine identifying information decrypted and extracted from user's PC by the transmission from the Toolbox."

The claims have been rejected as being unpatentable in view of the combination of Padgett and Ross. Applicant respectfully traverses the rejection. Padgett does not teach or suggest applicant's fingerprint file or applicant's means of authentication of a user machine.

Padgett is limited to positive user authentication and not authentication of a user machine. Applicant's invention requires both user identification plus a second form of authentication. This second form of authentication is not suggested by Padgett. Padgett is directed to a digital certificate based on biological indicia of the person providing the digital certificate so that the digital certificate provides a positive identification of the sender. As noted at Col. 2 of Padgett, line 54 the registrant

> "enters data corresponding to a biological or physical characteristic of himself, for example, his chromosomal DNA, into a terminal"

The Padgett patent also states that a photograph or scanned fingerprints, iris or retina can be used to create the digital certificate Col. 2, line 58-61. At col 4, line 14, Padgett describes how his digital certificate is formed.

> "A person wishing to obtain a certificate, hereinafter called the registrant, first visits a service provider to obtain a digitized representation of a biological characteristic of his or her body. This digitized characteristic will be referred to as a bio-blob. A bio-blob may be formed from, for example, a digitized image of the registrant's fingerprint, iris or retina or a digital representation of a marker plate prepared from the registrant's chromosomal DNA. Other physical characteristics may be used, depending on the degree of security desired. For example, an image of the registrant's footprint, handprint, dental x-ray or other distinguishing characteristic of the registrant's body may be used. The bio-blob may also be a combination of digitized images and other identifying indicia of the registrant and may include, for example, a password such as alphanumeric string. The service provider may be a medical clinic equipped to handle and analyze biological samples."

There is no suggestion of a second form of authentication in Padgett. To add a second form of identification to the Padgett system and eliminate the biological authentication that is so

central to the Padgett patent would destroy Padgett for its intended purpose. The whole focal point of a Padgett is the importance of a biological based data certificate to avoid fraud. The Summary of the Invention emphasizes the importance of biological and/or physical characteristics as the basis for a security where the inventor states:

> "It is an object of the present invention to provide a digital certificate for authenticating electronically transmitted documents which incorporates a unique characteristic of the sender, such as biological indicia that can only have come from the sender himself."

The importance of the biological indicia pervades the specification as Inventor stresses the importance of authenticating the user not anything else. The steps which Padgett takes to ensure that the user is the correct person are quite extensive. In Padgett, the user cannot participate in the security system of Padgett unless the user goes to, for example, a medical clinic where biological testing of biological samples must be performed on. The service provider gives the user a bio blob in digital form. A terminal must be used and this terminal must be owned or associated with the registrant. If a third party owns the terminal, then the device must be for the user's exclusive use. A public key and a private key are used for encrypting the data. When registering a bio blob, the user's bio blob is compared to existing bio blobs. When no match is found, the user is invited to register. The registrant goes to a remote terminal with the smart card containing the bio blob and the physical information. The physical information can be a registrant's driver's license, passport or other government issued identification card. Once registration is complete, the user information is stored for future verification.

If one skilled in the art were to ignore Padgett's biological authentication and modify it in an attempt to achieve applicant's invention the modified Padgett would still not suggest

applicant's invention because Padgett is only interested in authenticating the user and not anything else.

Security in Padgett relies on the bio blob and encryption. In the present invention there are dual security features. The first authenticates a user's identity. The second authenticates a user's computer. This is not suggested by Padgett. Padgett does not disclose a method of verifying a user and a user computer based on the hardware on the computer. A dedicated terminal is desired in Padgett because it restricts access to the encryption keys for the bio blob. There is no teaching or suggestion in Padgett of a fingerprint formed of anything other than the biological data. Applicant's claims are directed in general to a method for verifying a user and a user computer. Padgett only verifies a user through biological means and doe not verify a user's computer. Applicant's method includes the steps of receiving a request for verification from a computer and in response to the request for verification, sending at least one request to the user computer and receiving at least one response from the user computer. The at least one response includes a first fingerprint file and a first identification for the user. The first fingerprint file is not a biological characteristic file. Padgett does not include a fingerprint file that contains identifying characteristics of a user computer.

In applicant's invention, the first fingerprint file is compared to a second fingerprint file, to verify the user computer. The second fingerprint file is made up of identifying characteristics of a user computer. The first identification for the user is compared against a second identification for the user to verify the user, the second identification for the user accessible by the verification computer. At least one verification response is sent, based upon the

comparing of the first fingerprint file against the second fingerprint file and upon the comparing of the first identification for the user against the second identification for the user.

The Ross Patent also relied on by the Examiner relates to a fingerprint verification system, and it does not teach or suggest a method of verifying a user and a user computer. The fingerprint may be useful for verifying a user's identity, but the fingerprint is certainly not pertinent to verify both a user's identity and a user's computer. Ross claims it provides the capability of discriminating between real fingerprint data and counterfeit data by recognizing a degree of inexactness between respective scans of the same fingerprint. Ross focuses on a number of variables in making this determination. These variables include the inherent plasticity of the finger pressure applied by the finger on a scanning window, orientation of the finger on the window and the calibration and the precision of the scanner itself.

The combination of Ross and Padgett does not suggest Applicant's invention because such combination does not have an essential feature of Applicant's invention, the dual authentication. The present invention is directed to a method of entering into a secured transaction that is completely different from Padgett's biological digital certificate or Ross's fingerprint. With applicant's user and machine identification approach, users are limited to ONLY using machines that they are associated with, in order to conduct online transactions. Therefore, if they using a friend or family member's computer, or if they are on the road and using a hotel business lounge computer or an overseas kiosk, they WOULD NOT be able to use Applicant's "two-factor" security and would not be allowed to access a network or make a purchase, etc. online. This is not suggested by either of the cited references.

The present invention has particular applicability in situations where a user loses

personal data, such as a password. Under many prior art systems a user's identity can be used by unauthorized third parties. In the present invention, there is a second security feature that reduces the risk of fraudulent transactions - the fingerprint of the user's computer. It is very difficult for an unauthorized third party to make a fraudulent transaction with the present invention because it is difficult for the unauthorized user to get access to the user's computer.

CONCLUSION

For the foregoing reasons Applicant requests reconsideration of the rejection of the claims.

Respectfully submitted,

Thomas A. O'Rourke, Esq.
Bodner & O'Rourke, LLP
425 Broadhollow Road
Melville, New York 11747
Suite 108
(631) 249-7500

CERTIFICATE OF MAILING

I hereby certify that the foregoing documents were mailed by first class mail, postage prepaid, in an envelope addressed to the Hon. Commissioner for Patents P.O. Box 1450 Alexandria, VA 22313-1450 , this 31th day of August, 2004.

Thomas A. O'Rourke